PATENT ABSTRACTS OF JAPAN

(11)Publication number : 62-189593
(43)Date of publication of application : 19.08.1987

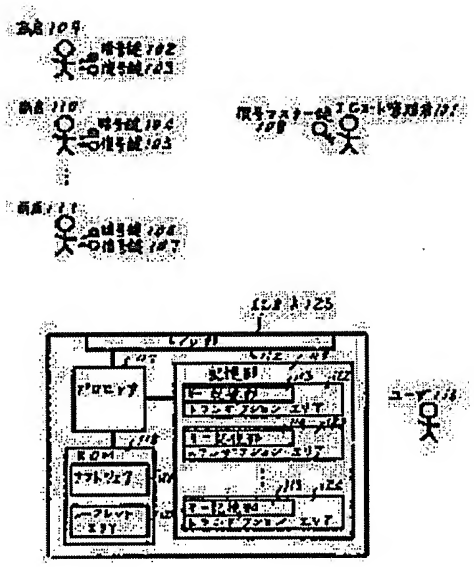
(51)Int.Cl. G06K 17/00
B42D 15/02
G06K 19/00

(21)Application number : 61-030815
(22)Date of filing : 17.02.1986

(71)Applicant : HITACHI LTD
(72)Inventor : TAKARAGI KAZUO
SHIRAISHI TAKAYOSHI
SASAKI RYOICHI

(54) IC CARD USING SYSTEM

(57)Abstract:
PURPOSE: To prevent the using condition concerning a certain commodity from being known for other commodity and to protect the privacy of a user by executing the writing to an IC card after the data such as the commodity name, amount, etc., are encoded by an encoding key different classified by the commodity at the time of using the IC card.
CONSTITUTION: An IC card controller 101 prepares pairs 102, 103, 104, 105, 106 and 107 of the coding key and the decoding key, prepares a master key 108 concerning decoding keys 103, 105 and 107 and holds them secretly at himself. Thereafter, the IC card controller 101 respectively transfers the pairs 102, 103, 104, 105, 106 and 107 of the coding key and the decoding key to commodities 109W111. Here, the writing of data to a memory part 119 and the reading of the data from the memory part 119 are executed by driving a processor 117 based on the control of a software 120 included in a ROM part 118 through an I/O part 112.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭62－189593

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和62年(1987)8月19日
G 06 K 17/00		T－6711－5B	
B 42 D 15/02		J－7008－2C	
G 06 K 19/00		R－6711－5B	審査請求　未請求　発明の数 3　（全8頁）

⑤4発明の名称　ＩＣカード利用システム

⑳特　願　昭61－30815
㉒出　願　昭61(1986)2月17日

⑦2発明者　宝木　和夫　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
⑦2発明者　白石　高義　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
⑦2発明者　佐々木　良一　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
⑦1出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
⑦4代理人　弁理士　小川　勝男　外1名

明　細　書

発明の名称　ＩＣカード利用システム

特許請求の範囲

1．データの書き込み／読み出し機能，および、データ処理機能を有するＩＣカードの利用システムにおいて、秘匿すべき相手が異なるデータは異なる暗号鍵で暗号化して記録しておき、ＩＣカード内の特定部分のデータの暗号化に用いた暗号鍵に対応する復号鍵のみを所望の相手に渡すことにより、上記特定部分のデータのみを上記相手が解読可能にすることを特徴とするＩＣカード利用システム。

2．前記復号鍵のすべてに対し、１つのマスター復号鍵が存在し、前記暗号文の各々は、該マスター復号鍵で復号化すれば元の平文に戻るという性質を利用して、該マスター復号鍵を有する者がＩＣカード内のすべてのデータを解読可能にすることを特徴とする第１項のＩＣカード利用システム。

3．前記秘匿部分の平文データには、該部分を暗号化、あるいは、復号化するための暗号鍵、あるいは、復号鍵が記述されており、通常は、該平文データは該暗号鍵で暗号化された暗号文の形で保持されており、ＩＣカードの外部で保持されていた暗号鍵、あるいは、復号鍵が紛失した場合には、該秘匿部分の暗号データをマスター復号鍵で復号化し記述内容を読み取ることにより、紛失した該暗号鍵、あるいは、復号鍵を再入手することを特徴とする第１項のＩＣカード利用システム。

4．データの書き込み／読み出し機能、および、データ処理機能を有するＩＣカードの利用システムにおいて、ＩＣカード内の、外部より直接読み出せない読みだし専用ファイル部にはセキュリテイコードをいれておき、データ破損検出部には保護すべきデータを上記セキュリテイコードと端末セキュリテイコードとを鍵として入力し、該データの破損を検出するデータ破損検出コードを該データに付加して、ＩＣカードファイル及び、取引先ファイルに保存することを

特徴とするＩＣカード利用システム。

5．上記取引先ファイルにたいし、取引先でのチエックとは独立に、ＩＣカードでのチエックをおこなうことを特徴とするＩＣカード利用システム。

6．データの書き込み／読み出し機能、および、データ処理機能を有するＩＣカードの利用システムにおいて、ＩＣカードの所有者が暗証符号を入力することにより、ＩＣカード内に記憶された各種データを取りだせるだけでなく、緊急時には、資格を有する第３者が、その識別符号と暗証符号を入力してＩＣカードあるいは記憶装置内の識別符号および暗証符号と合致すれば、指定されたデータ探索許可レベルに応じて、ＩＣカード内のデータの全部あるいは一部を読み出すことを特徴とするＩＣカード利用システム。

発明の詳細な説明

〔発明の利用分野〕

本発明は、電子ショッピング、電子小切手帳、クレジットカード等に係り、特に、取引者間におけるデータの破損、改竄等の防止に好適なＩＣカードを利用したシステムに関する。

〔発明の背景〕

プラスチックカードにＩＣ（集積回路）を埋め込んだＩＣカードは、個人確認、偽造困難、大容量記憶などの機能を有し、電子決済、パーソナル情報ファイル、セキュリテイ・コントロール等へ適用できる。

ところで、一枚のＩＣカードでスーパーマーケットや百貨店で買物をする場合、プライバシー保護の観点から、ある店で買つた買物リストは別の店で買物する時に読み出されないようにすることが望ましい。このため、ＩＣカード内に、店毎に異なるトランザクション・エリアを用意し、ある店は別の店のトランザクションを参照できないようにすることが望ましい。

従来技術の第１の問題点として、同一のＩＣカード内の複数個のトランザクション・エリアを異なる暗号鍵により保護する方式、および、そのために好適な鍵管理方式は提案されていなかつた。

一方、公開鍵暗号系のうち、ＲＳＡ法とRabin法には、マスター鍵が存在することが示されている。このマスター鍵を用いれば、前記の鍵管理を効率的に行うことができると考えられる。

従来技術の第２の問題点として、ＩＣカードの偽造、カード内データの破壊、改竄にたいする配慮がされていなかつた。

さらに、第３の問題点として、従来のＩＣカードは、単独の個人が利用することを前提とするものであつた。（「『ＩＣカード時代』は来るか」日経コンピュータ１９８５年７月８日号参照）。ところが、健康管理データ、資産管理データ等をＩＣカードに入力して利用しようとすると、本来の使用者が暗証番号をキーインして対象データの出力を行なうだけでなく、緊急時には医師や銀行員が別の暗証番号をキーインして、その対象データの全部または一部を出力したい場合も多い。

〔発明の目的〕

本発明の第１の目的は、ＩＣカードにおけるこのような従来の欠点を除去したうえでＩＣカード内のトランザクション・エリアのデータを保護する方式を提供することにある。

本発明の第２の目的は、キャッシュレス・ショッピング、クレジットカード等において、カードの偽造、カード内データなどのデータの破壊、改竄の検知方式を提供することにある。

本発明の第３の目的は、ＩＣカードの利用において、本来の使用者と緊急時に必要な人間がそれぞれに許された情報の出力を可能とすると共に、その他の人間からデータを保護する方式を提供することにある。

〔発明の概要〕

上記第１の目的を達成するため、本発明においてはＩＣカードのトランザクション・エリアへのデータの書き込み、読み出しにおいて以下の処理をおこなう点に第１の特徴がある。

1. ＩＣカード管理者は、事前に、秘匿すべきトランザクション・エリアの個数だけ暗号鍵、復号鍵の組を作成するとともに、該復号鍵すべて

に対するマスター復号鍵を一つ作成しておく。

2. ＩＣカード管理者は、各トランザクション・エリアに暗号鍵、復号鍵を１組ずつ割り当て、トランザクション・エリアの一部分に使用限度額、および、該暗号鍵、あるいは、復号鍵を書き込み、該暗号鍵で該トランザクション・エリアを暗号化しておく。

3. ＩＣカード管理者は、ユーザに該ＩＣカードを渡しておく。また、ＩＣカード管理者は、該暗号鍵、および、復号鍵を、各々の商店に渡しておき、各商店が、該トランザクション・エリアの暗号化、および、復号化を行えるようにしておく。

上記１～３により、商店毎に保持する暗号鍵、および、復号鍵は異なるので、ある商店はＩＣカード内の複数個のトランザクション・エリアのうち、保持する暗号鍵、復号鍵に対応するトランザクション・エリアしか意味のある処理はできない。これにより、ユーザのプライバシーは保護される。また、ＩＣカード管理者は、マスター復号鍵を保持するだけで、ＩＣカード内のすべてのトランザクション・エリアを任意に復号化し、内容を知ることができるので、個別の復号鍵の紛失対策に使用できる。さらに、マスター復号鍵は取引のときに使う必要はないので、安全に管理することができる。

また上記第２の目的を達成するため、データの破壊、改竄に関し、カード内データは、残金チェック及びデータ破損検出符号チェックにより検出し、販売店ファイル、銀行ファイルのデータ破損、改竄はデータ破損検出符号及びＩＣカードデータとの照合によりチェックする点に第２の特徴がある。

データ破損検出回路は、原理的には符号誤り検出回路のアルゴリズムに似ていて、暗号機を使用し出力を入力に帰還する事により実現できる。

さらに、上記第３の目的を達成するため、入力された暗証番号（番号だけでなく符号でも良い）によつて、ＩＣカードのマイクロプロセッサが、許容されたレベルを判定すると共に、アクセス可能なデータ領域を決定することにより、それぞれに許されたデータを出力する点に第３の特徴がある。

〔発明の実施例〕

第１図は、本発明の第１の実施例であるＩＣカード暗号システムの一構成例である。

先ず、前準備として、次を行う。

ＩＣカード管理者１０１は、暗号鍵、復号鍵の組（１０２，１０３），……，（１０６，１０７）を作成するとともに、復号鍵１０３，……，１０７については、それらのマスター鍵１０８を作成し、自分のところに秘匿して保持しておく。その後、ＩＣカード管理者１０１は、暗号鍵、復号鍵の組（１０２，１０３），……，（１０６，１０７）を商店１０９，……，１１１にそれぞれ渡しておく。さらに、ＩＣカード管理者は、ＩＣカード１１２の各キー記憶部１１３，……，１１５に暗号鍵、復号鍵の組（１０２，１０３），……，（１０６，１０７）をそれぞれ、１組ずつ書き込み、かつ、各トランザクション・エリア１２２，……，１２４に使用限度額を書き込んだ後、ＩＣカード１１２をユーザ１１６に渡しておく。ここで、記憶部１１９へのデータの書き込み、および、記憶部１１９からのデータの読み出しは、Ｉ／Ｏ部１１２を介し、ＲＯＭ部１１８に入つているソフトウエア１２０の制御のもとにプロセッサ１１７を駆動することにより行う。

第２図は、ユーザ１１６が商店１０９で買物を行うときの、本システムの処理フローである。

２０１：ユーザ１１６は、自分の暗証番号を、Ｉ／Ｏ部を介してプロセッサ１１７に入力する。

２０２：プロセッサ１１７は、ソフトウエア１２０による制御のもとに、シークレット・エリア１２１にある暗証番号を引き出す。

２０３：プロセッサ１１７は、ユーザ１１６が入力した暗証番号と、シークレット・エリアにある暗証番号が一致すれば、"ＯＫ"、一致しなければ、"ＮＯ"の信号をＩ／Ｏ部を介して外部に出力する。

２０４："ＮＯ"の信号が出力された場合、プ

ロセッサ１１７は、それ以降"ＯＫ"の信号が出力されるまで、データの書き込み、および、読み出しを行わない。

２０５："ＯＫ"の信号が出力された場合、商店１０９は、ユーザ116の買物の内容に応じて、暗号鍵１０２、および、復号鍵１０３を用いて、トランザクション・エリア１２２の内容の更新を行う。

つぎに、本発明の第２の実施例をＩＣカード利用によるショッピングシステムについて説明する。

このショッピングシステムにおける不正発生は、ＩＣカード内で、銀行よりの入金の改竄、売買データの改竄などが考えられる。

これを防止するためのＩＣカードブロック図を第３図に示す。

ＩＣカードは、パスワード等による本人確認を本人照合回路１で行つた後でないと次の動作に進めない。セキュリテイコード２は、直接外部から読むことができない読出し専用メモリである。銀行口座番号３は、読出し専用メモリに書き込まれている。データ破損検出回路は、第２図に示す様に、暗号機出力を入力に帰還させることによりデータ中に生じた誤りを検出することができる。即ち、データの各ビットの影響が順次後方に伝播するからデータの後にこの影響を受けたビットを適当な長さだけ対加して、データ破損検出符号とする。従つて、最初の正しいデータに対する付加符号とかりに改竄されたデータの検出符号は異なる事になる。

入出力回路５は、ＩＣカードとカード用端末とのインターフエース回路である。データファイル６は、入力時刻、販売店名、入出金、データ破損検出コード等のファイルである。

始めに、カードに入金を記入するとき、銀行端末にカードをセットしキーボードよりパスワードを入力する。パスワードは入力制御回路５を経て本人照合回路１にて回路内コードと照合し本人確認を行う。ＯＫならば照合回路１よりの信号により銀行口座番号が出力される。これにより銀行端末で口座ファイルがオープンされる。キーボードより入金データが入力されるとカードには、この入金、時刻、残金、端末番号等と共に端末の秘密符号が入力される。カード内では、入力制御回路を経たデータはデータ破損検出回路に送られる。データ破損検出回路において、カードのセキュリテイコードと端末のセキュリテイコードとを鍵として、時刻、端末番号、入金等を入力として暗号機に与えデータ破損検出符号を得る。これらをファイルに書き込むと同時に、銀行端末に送られさらに、銀行口座ファイルに書き込まれる。

商店にて買い物をする場合、本カードを売店端末に接続しパスワードを売店端末のキーボードより入力する。これが正しいとカードから売店端末は、残金を読みだすことができる。従つて、残金チエックの後、価格を端末のキーボードより入力する。カードでは、前と同様、出金、時刻、残金、売店端末番号等と共に端末の秘密の符号が入力されると、データ破損検出回路にて、カードと端末のセキュリテイコードを鍵として、時刻、端末番号、出金等を入力としてデータ破損検出符号を得る。これらをファイルに書き込むと同時に売店端末を経て売店ファイルに口座番号を含め書き込む。

売店ファイルは、銀行に配送され、口座番号毎に整理され銀行口座ファイルに書き込まれる。

残金が少なくなつて、再度カードに入金する場合、銀行端末にこのカードをセットしパスワードをいれる。パスワードＯＫであれば、銀行端末からカードのファイルの読みだしが可能になる。銀行端末は、カードから口座番号を読みだし口座ファイルをオープンする。口座ファイルは商店からのデータが既に記入されている。従つて、カードのファイルと口座ファイルとを照合することと残金チエックにより正、不正が判明する。

双方のレコードが正しいと、カードファイルから、そのレコードを消去する。

総てのレコードがＯＫとなれば、端末のキーボードより入金処理を行う。残金処理は、銀行内で行い、残金欄６４には、今回の入金を入出する。

残金チエックは、カードファイル最初の残金より逐次買い物による出金６３を引算しその結果と

残金６４を照合する事である。

レコードが不一致になつたとき等、各々について、そのレコードの端末番号６２により端末の秘密符号を銀行ファイルから読出し、これとレコードをカードに入力し、カードよりデータ破損検出符号を得る。この符号と先のカード又は銀行ファイルのレコードのデータ破損検出符号を照合することを、検出符号チエツクという。

今、あるレコードが不一致になり、その部位が時刻のとき、これらのレコードの何れかに一致する時刻のレコードをカードファイル及び銀行ファイルから探す。

a）ＩＣカードに該当レコード無し、銀行レコードの検出符号チエツク及び残金チエツクＯＫ、この場合は、カードのレコード抜けであり、ＩＣカードのレコードを消去したとみなされる。

b）ＩＣカードに該当レコード無し、銀行レコードの検出符号チエツク不合格、この場合は、銀行側のレコード付加であり、銀行ファイルに不正なレコードを追加したとみなされる。

銀行側レコードに該当レコードが無い場合についても同様に、判定できる。

次に、あるレコードが不一致になり、その部位が端末番号、入出金のとき、各々の検出符号チエツクによつて、正，不正が判明する。

また、あるレコードが不一致になり、その部位が残金のとき、各々の残金チエツクによつて、正，不正が判明する。

なお、時刻データの替わりに通し番号などの番号を使用しても良い。

以上、本実施例によればＩＣカード及び銀行ファイルデータ改竄検出の効果がある。

つぎに、本発明の第３の実施例を第５図～第７図により説明する。

第５図は、健康管理データ用ＩＣカードシステムの概略構成図を表わしている。ＩＣカード100は、接続部２９０を介して、ＩＣカード用端末２００に接続され、ＩＣカードとしての機能をはたす。

ＩＣカード１００は、マイクロプロセツサ120、ＲＯＭ（Read Only Memory）１１０、PROM（Programable Read Only Memory）130、EEROM（Electrically Erasable Read Only Memory）140から構成され、その間は信号線１５０で接続されている。ＩＣカード１００がＩＣカード用端末２００に接続されると、PROM１３０内のプログラムが、マイクロプロセツサ１２０内にロードされ、使用可能な状態となる。

ＩＣカード用端末２００は、マイクロコンピュータ２４０、キーボード２１０、ディスプレイ２３０より構成され、その間は信号線１５０でつながつている。また、マイクロコンピュータ240は信号線１５０、モデム３１０、公衆回線３２０、モデム３３０を介して、データ管理センタ４００につながつているものとする。同センタ４００はコンピュータ４１０とデータベース４２０よりなつている。

ＩＣカード１００の持ち主がかかりつけでない医師のところへ行つた場合、ＩＣカードの持主がキーボード２１０より正しく自分の暗証番号等を入力し、その信号は端末側のマイクロコンピュータ２４０を介して、ＩＣカード側のマイクロプロセツサ１２０に送られる。マイロプロセツサ120では、ＲＯＭ１１０の中を探索する。

ＲＯＭ１１０内は、第６図に示すようなデータ構成になつているものとする。すなわち、ＩＣカード１００の持ち主の暗証番号１１１、持ち主の情報探索許可レベル１１２、登録された各医師の医師免許コード１１３、暗証番号１１４、および情報探索許可レベル１１５、登録外医師に対する情報探索許可レベル１１６から成る。

マイクロプロセツサ１２０によるＲＯＭ１１０の中の探索により、入力された暗証番号が、持ち主の暗証番号１１１と合致するなら、その情報探索許可レベル１１２を読み出す。ここでは、レベル１だつたとする。マイクロプロセツサ１２０は、そのレベルに基づき、EEROM１４０内のデータファイルを読みに行く。

ＥＥＲＯＭ１４０内のデータ構造の一例を第７図

に示す。ここには、Aデータ（レベル1およびレベル2でアクセス可能）141とBデータ（レベル1のみアクセス可能）142が入つているものとする。例えば、Aデータ141には、血液型、健康診断結果、既応歴、等、診断，治療に必要なデータが入つている。またBデータ142には、家族構成等診断，治療には直接関係ないものや、どうしても本人の承諾なしには見せたくないものが入つているものとする。

この場合は、マイクロプロセッサ120により、レベル1が与えられているので、Aデータ141および、Bデータ142がアクセスされ、マイクロプロセッサ120から、端末用マイクロコンピュータ240に送られ、表示用処理を実施した後、ディスプレイ230に表示される。この表示は、医師にも見せられ診断，治療に生される。また、この結果の一部は、キーボード210より入力され、マイクロコンピュータ240、マイクロプロセッサ120等を介してEEROM140内のAデータ141あるいはBデータ142に書き込まれる。

もし、ICカード100の持ち主が、交通事故等で、緊急な治療を必要とし、かつ、本人が暗証番号を入力できないとする。この場合には、医師が医師免許コードと自分の暗証番号をキーボード210より入力する。この入力結果は、マイクロコンピュータ240を介して、ICカード100のマイクロプロセッサ120に送られる。マイクロプロセッサ120では、ROM110内の登録医師の医師免許コード113、暗証番号114と入力された医師免許コードおよび暗証番号を比較し、合致するものがあつたらその情報探索許可レベル115を読み出し、EEROM140内から、許可レベルに合つたデータを読み出す。その結果は、マイクロプロセッサ120、マイクロコンピュータ等を介してディスプレイ220上に表示される。

もし、対応するROM110上に医師免許コードは発見されたが暗証番号が合致しない場合は、そのことをディスプレイ220上に表示し、処理を完了する。

ROM110上に医師免許コードも発見できない場合は、医師により入力された医師免許コードおよび暗証番号は、データ管理センタ400に送られる。データ管理センタ400では、コンピュータ410を利用し、データベース中の医師免許コードと暗証番号に合致するものがあるかどうか照合する。両方合致するものがあれば、合致を表わす秘密のコードを、マイクロコンピュータ240等を介してICカード100に送り、ICカード100では、ROM110内の登録外医師に対する情報探索許可レベル116に応じてデータを取り出し、ディスプレイ220に表示する。

データ管理センタ400のデータベース420において、入力された医師の医師免許コードあるいは暗証番号が合致しない場合は、そのことをディスプレイ220に表示し、処理を完了する。

ここで、何度も入力することにより、偶然に一致する危険を避けるため、誤つた暗証番号の入力がM回（Mは指定）以上あつた場合にはアクセスを不可能にする等の対策をしておくことも可能である。更に、データ管理センタをアクセスした場合には、医師免許コード、その日時および、対象カードの持ち主等をセンタのデータベースにログとして残すことも考えられる。

また、ROM110とEEROM140の内容を分ける場合について記述したが、EEROM140にいつしよに保存することも可能である。更に、EEROMの替りに、データが消えないようにできるならRAM（Randam Access Memory）であつても良い。

上記実施例においては、情報探索許可レベルは2つの場合について説明したが、3つ以上に分けても良いことは言うまでもない。

また、健康管理データ用ICカードシステムについて説明したが、資産管理データ用ICカードシステム等、緊急時に資格を持つた第3者がデータをアクセスする必要があるものなら同様に実施することが可能である。

〔発明の効果〕

本発明により、金融機関等がＩＣカード管理者となり、ユーザに複数商店の利用を可能とするＩＣカードを発行するシステムにおいて、次の利点を得ることができる。

(1) プライバシーの保護：ＩＣカードの使用時に、商品名、金額等のデータは、商店別に異なる暗号鍵で暗号化された後、ＩＣカードに書き込まれる。このため、ある商店についての利用状況が他の商店に知られることはなく、ユーザのプライバシーは保護される。

(2) 鍵管理の容易性：ＩＣカード管理者は、ユーザ一人に対して、マスター復号鍵を一個持つだけで、ＩＣカードの全データを解読することができる。ＩＣカード管理者は、ＩＣカードに記録された使用額の決済をするときなどに、鍵管理の手間が少なくて済む。

(3) 鍵管理の安全性：マスター復号鍵は、ＩＣカード管理者のみが保管しているので、アクセス回数は比較的少ない。したがつて、マスター復号鍵は、安全に管理することができる。また、商店が何らかの事故により、暗号鍵、あるいは、復号鍵を紛失した場合、マスター復号鍵を用いてＩＣカード内の暗号鍵、あるいは復号鍵を容易に取り出すことができる。

(4) ＩＣカード及び銀行ファイルデータ破損、改竄検出ができる。

(5) ＩＣカードの持ち主以外も、資格を持つた第３者が、真に緊急時には、データをアクセスし利用することが可能である。

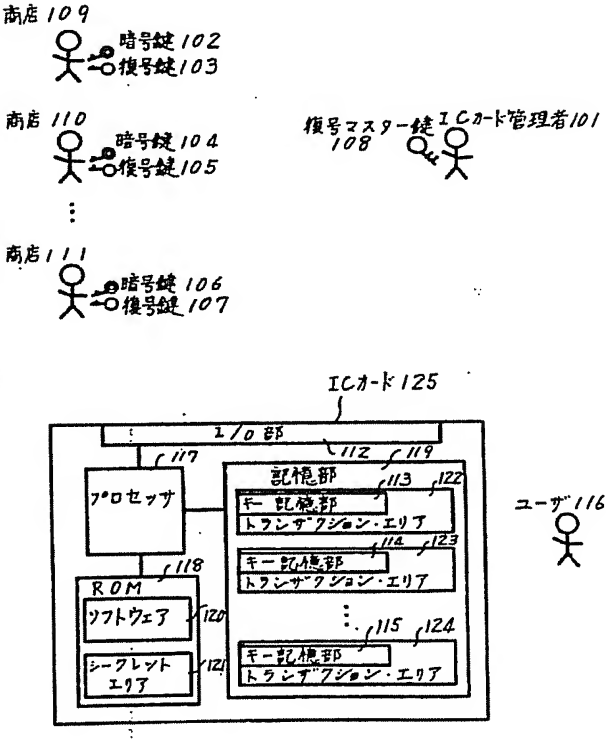
(6) ただし、データをアクセスできるレベルを分離し、そのレベルの範囲でしか取り出せないので、カードの持ち主がどうしても知られたくないデータは本人に無断で、第３者に知らせなくてすむ。

(7) 資格を持つた第３者は、カードに登録したものと、それ以外の管理センタに登録したものに階層化することにより、医師が利用する場合、常に、通信回線を利用してセンタへアクセスする手間およびコストを低減している。

図面の簡単な説明

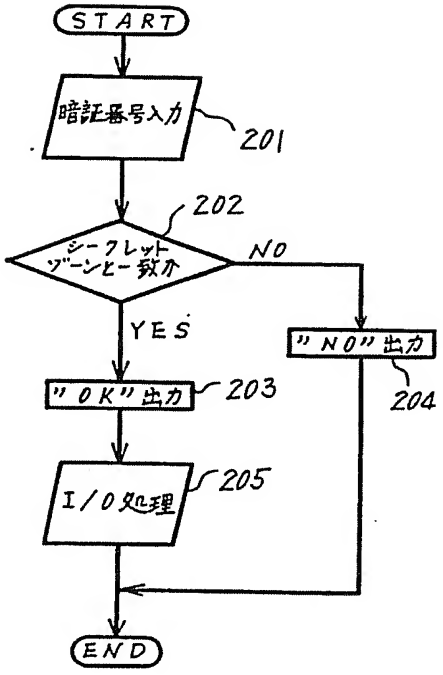
第１図は本発明の第１の実施例であるＩＣカード暗号システムのブロック構成図、第２図はユーザが、ＩＣカードを用いて、商店で買物を行うときの、ＩＣカード利用システムの動作フロー、第３図は本発明の第２の実施例であるショッピングシステムのブロック構成図、第４図はＩＣカードのデータ破損検出回路のブロック構成図、第５図は健康管理データ用ＩＣカードシステムのブロック構成図、第６図はＲＯＭ内データ構造の一例を示す図、第７図はEEROM内のデータ構造の一例を示す図である。

第　１　図

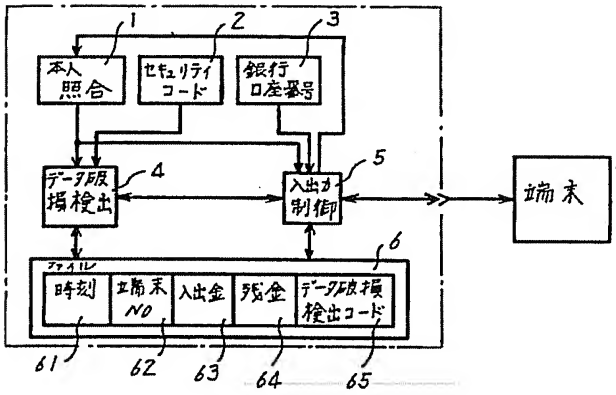


代理人　弁理士　小川勝男

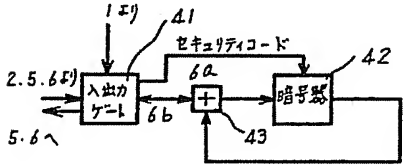
第 2 図



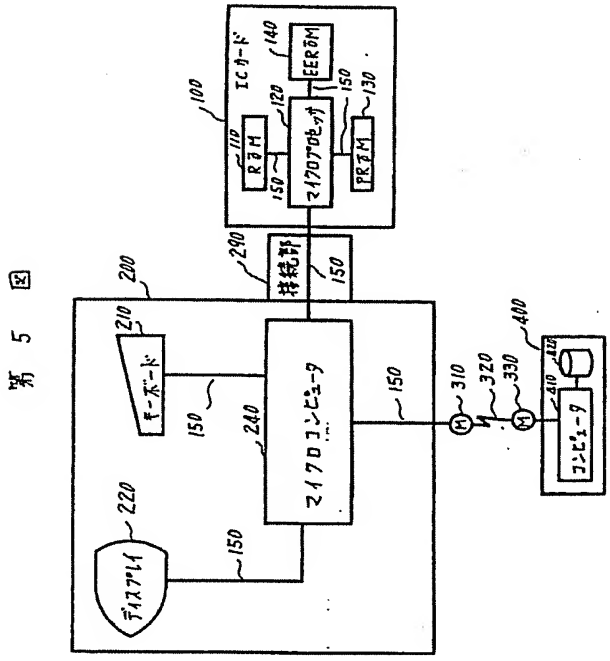
第 3 図



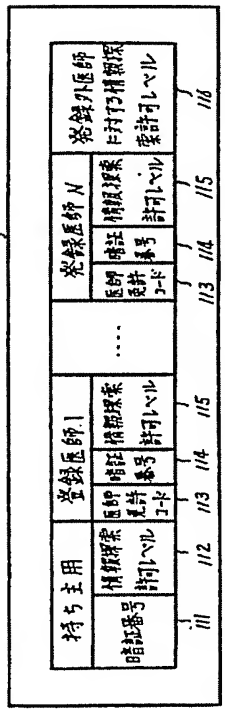
第 4 図



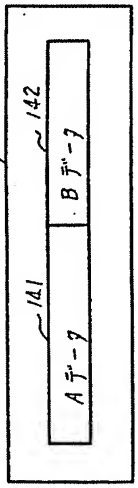
第 5 図



第 6 図



第 7 図



【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成６年（１９９４）１月２１日

【公開番号】特開昭６２－１８９５９３
【公開日】昭和６２年（１９８７）８月１９日
【年通号数】公開特許公報６２－１８９６
【出願番号】特願昭６１－３０８１５
【国際特許分類第５版】
G06K 17/00 T 7459-5L
B42D 15/10 521 9111-2C
G06K 19/10
G07C 9/00 Z 9146-3E
G07F 7/08
【ＦＩ】
G06K 19/00 R 8623-5L
G07F 7/08 G 7130-3E

手　続　補　正　書

平成 5 年 2 月 15 日

特許庁長官　殿

事件の表示
昭和６１年　特　許　願　第３０８１５号

発明の名称　ＩＣカード利用システム

補正をする者
事件との関係　特　許　出　願　人
名称　(510) 株式会社　日　立　製　作　所

代　理　人
居所　〒100　東京都千代田区丸の内一丁目５番１号
株式会社　日　立　製　作　所　内
電　話　東　京　3212－1111(大代表)
氏名　(6850) 弁理士　小　川　勝　男

補正の対象　明細書の特許請求の範囲の欄
補正の内容
１．本願明細書の特許請求の範囲を別紙の如く補正する。

別紙
特許請求の範囲
１．データ記憶手段とデータ処理手段と外部装置インターフェイス手段とを備えたＩＣカードを該カードの利用対象となる複数の外部装置のうちの任意の１つに接続し、上記外部装置が、上記ＩＣカード内のデータ処理手段を介して上記データ記憶手段へのデータの書き込みまたは読み出しを行うようにしたＩＣカード利用システムにおいて、上記各外部装置に予め１組の暗号鍵と復号鍵とを割当て、上記データ記憶手段に複数の暗号鍵または復号鍵と対応する複数のデータ記憶領域を定義しておき、上記ＩＣカードと接続された各外部装置が、上記複数のデータ記憶領域のうち、該外部装置の暗号鍵または復号鍵と対応する特定のデータ記憶領域において、上記暗号鍵で暗号化されたデータの読み出しまたは書き込みを行うようにしたことを特徴とするＩＣカード利用システム。
２．前記ＩＣカードのデータ記憶手段が、該ＩＣカードの利用者に固有の暗証情報を記憶しており、

上記ＩＣカードを前記外部装置に接続した状態で、前記データ処理手段が利用者の入力した暗証情報と上記記憶してある暗証情報との対応関係をチェックし、入力暗証情報の正当性が確認された場合にのみ上記外部装置から前記特定データ領域のデータの読み出しまたは書き込みを可能とするようにしたことを特徴とする第１項に記載のＩＣカード利用システム。